السيبرانيّة: الحرب الخفيّة في المنطقة المظلمة

د. رولا حطيط*

المقدّمة

منذ بدء ثورة المعلومات الرقميّة التي تجلّت في انتشار شبكة الإنترنت، زاد اعتماد الدول والمجموعات والأفراد عليها. وهذه الثورة لم يقتصر مداها على الاستفادة من تقنيّات دمج الصوت والصورة، ولم تعد مجرد أداة اتصال وتواصل بين طرفين محدّدين، بل باتت بحكم انفتاحها ومرونة الإبحار داخلها، «وسطًا» تعتمل في «فضائه» البوّابات والمواقع والمدوّنات، لا بل الحروب الإلكترونيّة، جرّاء استحداث برامج إلكترونيّة معدّة لأغراض عسكريّة أو تطويرها، تُعرف اختصارًا بالسايبر (cyber)[1]. وترسم ملامح الحروب في القرن القادم حروب خفيّة تقاد في الظلّ، من خلال شاشة حاسوب، غيّرت الواقع وفرضت سيطرة عالميّة من نوع جديد، إذ يبدو الأمر وكأنّه فيلم خيالٍ علميّ أبدعت هوليوود في إخراجه؛ ولكن نحن في القرن الـ21، وقد أصبح الأمر ممكنًا بشكل يصعب تصديقه، فلم يعد الأمر مقتصرًا على الأفلام بل صار حقيقة والسلاح معلومة، أمّا الفضاء فهو قائم على التكنولوجيا؛ إنّها قوّة جديدة فاقت بهدوئها الحرب الباردة، وأدخلت للساحة جنودًا غير مرئيّين، وهذا يستلزم تغيير الاستراتيجيّة في اتجاه التصعيد مع قوى أخرى معادية نشطة في ساحة الحرب السيبرانيّة، أو ما عُرف بحرب الأصفار والآحاد التي تحاربت عليها منذ أكثر من عشرة أعوام فرق من القوّات الخاصّة للدول الكبرى ومجموعات من قراصنة المعلومات[2] المجنّدين حسب اللزوم، ما يشكّل

---

* باحثة لبنانية.

[1]– هناك عدد من الترجمات العربيّة لمصطلح ، Cyberمنها: المعلوماتي، والافتراضي، والسيبراني، والرقمي؛ غير أنّه في هذا البحث تم استخدام لفظ "سيبراني" بوصفه الترجمة الأقرب إلى الكلمة الإنجليزية

[2] –الهاكرز: لقب يُطلق على كلّ من هو عبقري خبير في الحواسيب

والأنونيموس: هي مجموعة قليلة تعمل في مجال الاختراق البرمجي؛ ومع بداية عام 2008م أصبحت جماعات الأنونيموس مُتعلقة بشكل متزايد بالعمل الجماعي العالمي للاختراق.

الكراكرز: هم أناس يخترقون الحواسيب الشخصي وغيرها من حواسيب الشركات.. إلخ، ومن أسباب الاقتحام: أسباب مادية كسرقة نقود من بنك، أو سرقة أموال من حساب شخص ما وتحويله الى حساب المخترق، أو للهواية، أو لإبراز

أحد أهمّ التحدّيات الراهنة، وبالأخصّ في تحديد طبيعتها أو عناصرها، فضلًا عمّا يترتب عليها من تبعات، سيّما أنّها حرب المستقبل؛ وهي من أخطر الحروب التي تختلف عن كلّ الأجيال السابقة من الحروب كونها مجهولة من حيث جهة الهجمة أو هدفها. كما وتفاجأ بها الدولة المستهدفة بعد حدوثها.

فما هي الحروب السيبرانيّة؟ كيف نشأت؟ ومن يشغّلها؟ هل يمكن أن تُصنّف ضمن وسائل القتال وطرقها؟ أيّ تغيير أحدثته الهجمات السيبرانيّة على مفهومَي القوّة والصراع في عالمنا الحديث؟ وماذا عن حدود المواجهات الأبرز بين الولايات المتحدة الأمريكية و«إسرائيل» من جهة وإيران من جهة ثانية؟ وما هي استراتيجيّات الدول لحماية أمنها في عصر الفضاء السيبراني؟ وهل الاستراتيجيّات الكلاسيكيّة كافية لمواجهة الهجمات السيبرانيّة؟ إشكاليّات كثيرة تُطرح، سوف نحاول في هذا البحث مقاربة أهمها.

فهذا البحث يهدف في مقاربة موضوع الحرب السيبرانيّة إلى توعية الناس لخطورة هذه الحرب، وضرورة الاستعداد والتصدّي لها. والأمر يبدأ من الفرد وليس فقط من الدولة، في ظلّ تنامي استخدام الأفراد اللامتناهي لتكنولوجيا المعلومات والاتّصالات والاعتماد عليها بشكل أساسي، ما يستوجب تنمية قدرات المواطنين وبناءها في هذا الشأن، وخاصّة أنّها، بحكم مستوى تقدّمها المتعثر، لا تستطيع مواكبة التطوّر السريع في وسائل التكنولوجيا الحديثة والاتصالات؛ لذلك فهي تعاني سلبيّاتها فقط. من هنا لا بدّ من مقاربة الموضوع بدءًا بالتعريفات العامّة، ومن ثم الإجابة عن تساؤلات البحث، لكي يكون الموضوع في متناول شريحة كبيرة من القرّاء.

أوّلًا: السيبرانيّة (لغة واصطلاحًا)

من أجل الوقوف على مفهوم السيبرانيّة، سنبحث في نطاق تعريفها لغةَ واصطلاحًا في ضوء المعاجم اللغويّة، وما أدرجه المختصّون في القانون الدوليّ العام، وخبراء تكنولوجيا المعلومات.

أ- في اللغة

القدرات والتفاخ، مثل طلاب الجامعات الذين يدرسون البرمجة ويخترقون حواسيب بعضهم للتفاخر بالقدرة على الاختراق . والكراكرز درجات، فمنهم الخبير: وهو يستطيع أن يتحكم بالجهاز بالكامل ويمكنه تحريك الماوس دون أن تحرّكه أنت ويستطيع أن يمحو كل مجلّداتك أو أي أشياء تخصّك؛ والمبتدئ: وهو أكثر خطرًا من الخبير، لأنه غير مجيد للاختراق، ولا يعرف ما يفعل، ويمكن أن يمحو أو يحدث مشاكل في نظام التشغيل الخاص بك لا يمكن إصلاحها بسرعة.

كلمة سايبر (Cyber) يونانيّة الأصل، وترجع إلى مصطلح «kybernetes» الذي ورد بداية في مؤلّفات الخيال العلميّ، ويعني القيادة أو التحكّم عن بعد[3].

والسيبرانيّة في قاموس (المورد) هي علم الضبط ، ومصدرها (Cybernetics)[4]، وهو مصدر يتطابق مع مفهوم الهجمات السيبرانيّة، أي ضبط الأشياء عن بُعد والسيطرة عليها.

إن أوّل من استخدم مصطلح السيبرانيّة هو عالم الرياضيّات **نوربرت وينر** (Norbert wiener)، وذلك في العام ١٩٤٨، في أثناء دراسته موضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلًا عن حقل الهندسة الميكانيكية[5].

وبالرجوع إلى المختصّين في اللغة العربيّة، نجد أنّ ثمّة تحديًّا يواجهونه في اختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الإنجليزية، لعدم وجود مصطلح مناظر له في اللغة العربيّة. بيد أنّ الترجمة العربية لعنوان اتفاقيّة مجلس أوروبا المتعلقة بالجريمة السيبرانيّة كانت ترجمة صائبة، إذ تُرجِم العنوان (Cybercrime on Conven) إلى اللغة العربيّة: (الاتفاقيّة المتعلّقة بالجريمة الإلكترونيّة)[6].

فيما عرّف قاموس مصطلحات الأمن المعلوماتيّ مصطلح السيبرانيّة بالقول: «هجوم عبر الفضاء الإلكترونيّ يهدف إلى السيطرة على مواقع إلكترونيّة أو بنى محمية إلكترونيّا، لتعطيلها أو تدميرها أو الإضرار بها»[7].

أمّا سبب اعتماد هذا البحث «مصطلحَ السيبرانيّة» الذي استخدمه نوربرت وينر في كتابه الذي ذكرناه سابقا (Cybernetic) ، فهو لعدم وجود مصطلح متفق عليه في اللغة العربيّة من جهة، ولأنّ الوثائق الصادرة عن الأمم المتحدة باللغة العربيّة استخدمت مصطلح «السيبرانيّة» ذاته من جهة أخرى[8].

---

[3] – Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University Press, 2010.

[4] –منير البعلبكي،" المورد: قاموس إنكليزي –عربي"، دار العلم للملايين، بيروت، 2004 ص 234

[5] –Norbert Wiener, "Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.

[6] – مجلس أوروبا،" اتفاقية مجلس أوروبا المتعلق بالجريمة الإلكترونيّة"، مجموعة المعاهدات الأوروبية رقم 185، بودابست عام 2001.

[7] –Richard Kissel, “Glassory of Key Information Security Terms", National Institute of Standards and technology, U.S Department of Commerce ", Revision, 2, May, 2013, p.57

[8] – يُنظر على سبيل المثال: مكتب الأمم المتحدة المعني بالمخدرات والجريمة: "تقرير الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها" ، فيينّا عام 2013 ، الوثيقةUNODC/CCPCJ/EG.4/2013/2 :

ب-اصطلاحًا

تبرز عدّة مصطلحات حول موضوع البحث؛ فنجد مصطلح الهجمات السيبرانيّة (Cyber Attack) ، ومنهم من تبنّى مصطلح الفضاء السيبرانيّ[9] (Cyber Space) ، بالاستناد إلى المحيط الذي تجري فيه العمليّات السيبرانيّة الناشئة عن أداء أنظمة إلكترونيّة مهمّتها تتبّع المعلومات التي تعمل إلكترونيّا وجمعها وتحليلها، ومن ثمّ اتخاذ إجراءات محدّدة لمهاجمتها عن طريق أنظمة إلكترونيّة أخرى مخصّصة لهذا الغرض[10]. وتبنّى آخرون مصطلح الحرب السيبرانيّة (Cyber Warfare) بالاستناد إلى أيديولوجيا أمنيّة أو عسكريّة تضع منهاجًا لتحقيق أهداف على الصعيد الأمنيّ أو العسكريّ تجاه (العدو المفترض)[11]. وفي هذا البحث سوف نعتمد مصطلح «الهجمات السيبرانيّة» كونها أقرب إلى الواقع الحالي المعاش على مستوى الدول؛ فالمقصود بالهجمات السيبرانيّة – وهو أشهر تعريف لها- «أنّها الأفعال الصادرة من أجهزة الحاسوب وشبكات المعلومات التابعة لدولة ما بشكل منظّم ومدروس على أجهزة حاسوب وشبكات معلومات لدولة أخرى، بغرض التجسّس[12]Espionage ، أو التخريب Sabotage [13]، أو التوجيه[14]».

---

[9] – يخلط البعض بين الفضاء الإلكترونيّ والإنترنت، في حين أن الانترنت هو الوسيط الذى تقوم من خلاله بتلبية جميع أغراضك المتعددة، ما بين شراء الكتب من موقع أمازون ومتابعة بعض الأفلام وغيرها... والعديد من الخدمات المقدّمة من شركة مايكروسوفت متاحة على الإنترنت، والبرامج المختلفة والخدمات متاحة على الإنترنت أيضاً؛ ولكن الفضاء الإلكترونيّ أبعد من ذلك، على الرغم أنّ بُنيته أساسها الإنترنت، ولكنه أكثر ثراءً؛ وأصبح الفضاء الإلكترونيّ مجتمعًا يتفاعل فيه المواطنين عن طريق الشبكات، ولا يوجد خط فاصل بين الفضاء الإلكترونيّ والإنترنت، ولكن معيار التفرقة، يكون بحكم الخبرة والتعاملات والفئة العمرية . **لورنس لسيج ، الكود المنظّم للفضاء الإلكترونيّ ، ترجمة : محمد سعد طنطاوي ، ط 2 (القاهرة : مؤسسة هنداوي للتعليم والثقافة ، 2006) ص 31.**

[10] –James A. Lewis, "Sovereignty and the role of Government in Cyberspace", Center for Strategic and International Studies Journal, Spring Summer, Vol: XVI, Issue II, 2010, P.56.

[11] –Shin, Beomchul," The Cyber Warfare and the Right of Self –Defense: Legal Perspectives and the Case of the United States, IFANS, Vol.19, No1, June 2011, p.104

[12]– تُستخدم طرق غير شرعية لتعطيل عمل الشبكات العنكبوتية وحواسيبها، وأنظمتها بهدف سرقة معلومات سرّية من مؤسسات الخصم أو الأفراد ونقلها إلى الصديق السياسي، أو العسكري أو المالي.

[13]– قد تتعرض حواسيب الأنظمة العسكرية والمالية لخطر التخريب بهدف تعطيل عملياتها الطبيعية وتجهيزاتها.

[14] K.Saalbach," Cyber War, Methods and Practice", Version 9.0, University of Osnabruck- 17 Jun 2014, p.6-

ومن الممكن أن تكون الهجمات السيبرانيّة وسيلة وطريقة في الوقت نفسه. وبعبارة أخرى، يعتمد ذلك على الهدف من استخدامها؛ فقد تُسهم في توجيه العمليّات العسكريّة الأخرى، كالصواريخ بعيدة المدى أو الطائرات من دون طيّار (Drawn) ، لتحديد أهداف عسكريّة منتخبة وتدميرها، أو لتعطيل أجهزة الكشف المبكر للهجمات التي يقوم بها سلاح جوّ معادٍ، أو وقف عمليّات الاتصال في المطارات العسكريّة أو المدنيّة (الهجوم الذي قامت به «إسرائيل» عام 2007 على سوريا، إذ توقفت أجهزة الرادار وباقي منظومات الاتصال في المطارات العسكريّة والمدنيّة عن العمل في أثناء الهجوم الذي نفّذه سلاح الجو التابع لها على مواقع سوريّة زعمت إسرائيل أنّها منشآت؛ و في هذه الحالة يُعدّ الهجوم السيبرانيّ طريقة قتالية، إذ يدخل ضمن الخطط العسكريّة لمفاعل نوويّ، وبالتالي هو طريقة قتاليّة)[15].

وعلى العكس، قد تكون الهجمات السيبرانيّة وسيلة قتاليّة من خلال استخدامها بذاتها للتسلّل إلى أنظمة إلكترونيّة مُعدّة لحماية أو لتنظيم سير عمل منشآت حيوية، كمحطات توليد الطاقة النووية أو السدود أو وسائل النقل كالمطارات، بهدف تطويعها والسيطرة عليها، لتدمير ذاتها بذاتها من خلال تغذيتها بمعلومات خاطئة لأجهزة التحكّم والحماية الإلكترونيّة (ما تعرّضت إليه محطة (نطانز) النوويّة الإيرانيّة من هجوم سيبراني عام 2009، وأعلنت عنه الولايات المتحدة في العام 2011، إذ استخدمت برنامجًا يُدعى (Stuxnet) ، عطّل بعضًا من العمليّات الحسّاسة وألحق أضرارًا جزئيّة في عمليّات تخصيب اليورانيوم؛ وهو ما يمكن معه عدّ هذا الهجوم سابقة في حقل الهجمات السيبرانيّة)[16].

إنّما يعتمد التمييز بين وسائل القتال وطرائقه على الهدف من استخدامها والنتيجة التي ستؤدّيها. فكلّما كانت تتسبّب بطريق مباشر أو غير مباشر بقتل أو جرح أو تدمير أو تعطيل كلّي أو جزئيّ، عُدّت وسيلة قتاليّة؛ أمّا إذا استُخدمت كجزء من مخطّط عسكريّ فتُعدّ طريقة قتاليّة تخضع للنظام القانونيّ الدوليّ[17]؛ وهو ما تتّصف به الهجمات السيبرانيّة في الاثنين معًا.

ثانيًا: طرائق الهجمات السيبرانيّة

---

[15] – Thomas Rid and Peter Mcburney, op.cit, P.6

[16] –Michael Gervais, “Cyber Attacks and the Laws of War", Berkeley Journal of International Law", Vol: 30, Issue .2, Article 6, 2012, p.46

[17] –عرّفت المادة (51) من البروتوكول الإضافي الأول للقانون الدولي لعام 1977، الهجوم المسلّح على نحوين اثنين؛ الأول في 35 الفقرة (5/أ)، ويشير إلى الوسيلة القتالية: والهجوم قصفاً بالقنابل أياً كانت الطرق والوسائل....)؛ أما الثاني، فيشير إلى طريقة القتال؛، وذلك في الفقرة (5/ب):(والهجوم الذي يمكن أن يتوقع منه أن يسبّب خسارة في أرواح المدنيين أو يوقع إصابات بهم أو أضراراً بالأعيان المدنية...).

تعتمد الهجمات السيبرانيّة أساساً على الوحدات السيبرانيّة التي تضمّ الجنود السيبرانيّين، وهم في الأصل قراصنة رقميّون يتمّ استخدامهم على شكل فرق متخصّصة، وإعطاءهم إمكانات لوجستيّة وسيرفرات على شبكات المعلومات، وتوجيههم لأغراض محدّدة، مثل مراقبة كلّ شبكات المعلومات الحسّاسة (شبكات الطاقة، المياه، الكهرباء، الاتصالات، الأمور الماليّة في البنوك..)، أو الردّ على أيّ هجمات، أو التجسّس، أو توجيه رأي العام لدول معادية. وكانت معظم الهجمات الإلكترونيّة سابقًا تُشنّ بواسطة أشخاص أو مبرمجين لأهداف شخصيّة؛ أمّا في العقدين الأخيرين، فقد دخلت المنظّمات الأمنيّة والحكومات إلى هذه الساحة، وأخذت تُنفق الملايين لتطوير قدراتها وبناء جيوش إلكترونيّة للدفاع عن منشآتها وشنّ الهجمات المضادّة. وبرزت «إسرائيل» وأمريكا والصين وروسيا وإيران والمملكة المتّحدة وكوريا الشماليّة وفرنسا في مقدّمة الدول المتقدّمة في تقنيّات الحرب الإلكترونيّة.

تنقسم الهجمات السيبرانيّة الى نوعين رئيسين:

1- هجمات تعطيل جهاز الكمبيوتر المستهدف.

2- هجمات يكون الغرض منها الوصول إلى بيانات جهاز الكمبيوتر المستهدف، وربما الحصول على امتيازات المسؤول عنه.

ومن طرائق الهجمات السيبرانيّة نذكر:

- الطريقة الأولى:

إرسال روابط بشكل واسع عن طريق برامج التراسل لعدّة مستخدمين. وتعزَّز هذه الرسائل بخاصيّة تتيح التحكّم بحساب كلّ من يفتحها، حيث تمكّن القراصنة الإلكترونيّين من الوصول إلى بيانات المستخدمين وحساباتهم المصرفيّة حتى، أو كلمات سرّ تابعة لهيئات حكوميّة رسميّة.

- الطريقة الثانية:

أن يُجهّز الهاكر عدّة سيرفرات سريعة تقوم بإرسال ملايين الطلبات بوقت واحد إلى موقع أو عدّة مواقع إلكترونيّة، ما يؤدّي إلى توقّف عملها. وهذا يكلّف خسائر ماليّة، خصوصًا إذا كانت هذه الخدمات المقدّمة حكوميّة أو تابعة لهيئات ماليّة حيويّة؛ فيجري استهداف البنوك أو المواقع الحكوميّة التي تحتوي على بيانات مهمّة، أو حتى استهداف منشآت صناعية.

- الطريقة الثالثة:

أن يُنشِئ الهاكر مواقع بأسماء تكون قريبة جدًا من أسماء مواقع عالميّة موثوقة، مثل apple أو google، ويُرسل emails يطلب فيها فحص كلمة السرّ أو تغييرها، فيظنّ المستخدم أنّها الشركة

العالميّة ذاتها. وبمجرّد وضعه كلمة السرّ يتحكّم الهاكر ببياناته الخاصّة؛ وهذا له تأثير كبير إذا تمّ على مستوى الدول.

ثالثًا: مميّزات الهجمات السيبرانيّة

1- تستطيع الهجمات السيبرانيّة إلحاق الأضرار بالخصم، مهما كانت طبيعتها، من دون أن تتجاوز الحدّ الفاصل بين الحرب والسلام بشكل رسميّ.
2- صعوبة تحديد مصدرها وكلفته، إذ لا تعلن عنها الدولة المنفّذة غالبًا أو حتى الدولة المستهدفة، فتبقى مجهولة المصدر لأوقات طويلة، حيث إنّ تحديد مصدرها يحتاج إلى تتبّع وعمل من فرق متخصّصة.
3- يزول العامل الجغرافي في الهجمات السيبرانيّة، بحيث يصبح أيّ مركز أو منشأة عُرضة للاستهداف. ولا يقتصر على الأرض بل يصل التهديد إلى الفضاء، عبر إرسال الفايروسات إلى الأقمار الصناعية لتعطيلها أو سرقة البيانات منها.
4- الهجمات السيبرانيّة أقلّ كلفة من الحروب التقليديّة، وهي عامل مساعد فاعل بها، وتُعدّ أكثر أنواع المواجهة التي تعبّر عن حروب الجيل الخامس، لأنّها تشمل عمليّة التحكم عن بعد وتقنيّات الاتصال الجديدة.
5- إنّها تهديد وفرصة على نحو تبادليّ؛ فهي أداة للتجسّس، وسلاح للحرب، يستطيع الخصوم استخدامها لإلحاق الأذى بالخصم، ويستطيع الخصم أيضًا استخدامها لإلحاق الأذى بخصومه.
6- مؤثرة في السياسة والاقتصاد على الصعيد الدوليّ، نتيجة انتقال جزء كبير من الصراعات بين القوى العظمى في العالم إلى شبكة الإنترنت والوسط الرقميّ، مع تزايد ارتباط العالم بالفضاء الإلكترونيّ، تزامنًا مع تراجع دور الدولة في ظلّ العولمة وانسحابها من بعض القطاعات الاستراتيجيّة لمصلحة القطاع الخاصّ. وفي الوقت عينه، تصاعدت أدوار الشركات متعدّدة الجنسيّات، خاصّة العاملة في مجال التكنولوجيا.
7- ثمّة إمكانيّة لتسبّب الهجمات السيبرانية خسائر ماليّة ضخمة، وقد تُفضي إلى خسائر في الأرواح إذا تجاوزت قطاعات حسّاسة جدًّا، مثل أنظمة المستشفيات، وأنظمة التبريد في المفاعلات النوويّة.
8- لا يسبقها أيّ مؤشّرات، بمعنى أنّها من الممكن أن تحدث في أيّ وقتٍ وفي أيّ مكان، وبتأثير سريع جدًّا.

رابعًا: الصراع الدوليّ السيبرانيّ: بين النشأة والنماذج

بات الفضاء السيبرانيّ أحد العناصر الأساسيّة التي تؤثّر في النظام الدولي، بما يتيحه من أدوات تكنولوجيّة مهمّة لعمليّات الحشد والتعبئة في العالم، هذا بالإضافة إلى تأثيره في القيم السياسيّة. ونتيجة لسهولة الاستخدام ورخص التكلفة، زادت قدرته على التأثير في مختلف مجالات الحياة، سواء السياسيّة، الاقتصاديّة، العسكريّة، الاجتماعيّة وحتى الأيديولوجيّة؛ وبات جليًّا أنّ من يمتلك آليّات توظيف البيئة السيبرانيّة يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

ومن الأمور المتعارف عليها في العلاقات الدوليّة أنّ مصادر قوّة الدولة وأشكالها تتغيّر. فإلى جانب القوّة الصلبة، ممثّلة في القدرات العسكريّة والاقتصاديّة، تزايد الاهتمام بالأبعاد غير الماديّة للقوّة، ومن ثمّ بروز القوّة الناعمة التي تعتمد على جاذبية النموذج والإقناع. ومع ثورة المعلومات، ظهر شكل جديد من أشكال القوّة هو قوة السايبر (power Cyber)؛ ويُعدّ جوزيف ناي (Nye. Joseph) من أبرز المهتمين بالقوة، السيبرانيّة، حيث يُعرّفها بأنّها: «القدرة على الحصول على النتائج المرجوّة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبرانيّ؛ أي أنّها القدرة على استخدام الفضاء السيبرانيّ لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيليّة الأخرى، وذلك عبر أدوات سيبرانيّة»[18]. كما يوضح «ناي» أنّ مفهوم القوّة السيبرانيّة يشير إلى مجموعة الموارد المتعلّقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونيّة والبنية التحتية المعلوماتيّة والمهارات البشريّة المدربة للتعامل مع هذه الوسائل، والتي لها تأثير كبير في المستوى الدوليّ والمحليّ؛ فمن ناحية، أدّت إلى توزيع القوّة وانتشارها بين عدد أكبر من الفاعلين ما جعل قدرة الدولة على السيطرة موضع شكّ؛ ومن ناحية أخرى، منحت الفاعلين الأصغر قدرة أكبر على ممارسة كلّ من القوّة الصلبة والقوّة الناعمة عبر الفضاء السيبرانيّ، وهو ما يعني تغيّرًا في علاقات القوى في السياسة الدوليّة.

الجدير ذكره أنّ التسلّلات ليست بالأمر الجديد.، فبقدر قِدم العصور الرومانيّة، كانت الجيوش تعترض اتصالات العدو. في الحرب الأهلية الأمريكيّة[19]، استخدم جنرالات الاتحاديّين والكونفدراليّين (الانفصاليّين) أجهزة التلغراف الجديدة لإرسال أوامر مزيّفة إلى العدو. وأثناء الحرب العالميّة الثانية[20]، كسر خبراء التشفير البريطانيّون والأمريكيّون رموز الشيفرة الألمانيّة واليابانيّة، وكان هذا عنصرًا أساسيًّا في انتصار الحلفاء (ظلّ بعد ذلك سرًّا طوال أعوام كثيرة). وفي العقود القليلة الأولى

---

18 – Joseph S.Nye JR , Cyber Power, Harvard Kennedy School, 2010, P 30 .

19 – Edward J. Glantz, “Guide to Civil War Intelligence,” The Intelligencer: Journal of U.S. Intelligence Studies (Winter/Spring 2011), p.57

20 – David Kahn, The Codebreakers (New York: Scribner; rev. ed., 1996), Ch. 14 .P8.

من الحرب الباردة أيضًا، كان الجواسيس الأمريكيّون والروس يعترضون على نحو دوريّ ومنتظم اتصالات بعضهم ببعض من إشارات راديويّة (لاسلكية)، وبثّ للموجات الميكرويّة (الميكروويف) ، واتصالات هاتفيّة. ولم يقتصر الهدف على جمع معلومات استخباراتيّة بشأن نيّات الطرف الآخر وقدراته، بل إضافة إلى ذلك، الحصول على أفضليّة في الحرب الجسيمة المخيفة المقبلة.

أ- النشأة:

ثمّة من يجد أنّ أفكار الهجمات السيبرانيّة بدأت في أمريكا منذ الثمانينيّات خلال عهد الرئيس رونالد ريغان، الذي رأى أنّه من الممكن أن تتعرّض بلاده لخطر مثل هذه الهجمات، فأفرز فكرة مميّزة وسابقة لأوانها، أنتجت «وحدة السياسة القوميّة بشأن الاتصالات وأمن نُظم المعلومات»، التي تطوّرت خلال التسعينيات، واستخدمها الجيش في عمليّات الاستشعار عن بُعد؛، وظهرت الحاجة إليها وإلى تقنيّاتها خلال «الحرب على العراق في 2003»[21].

كانت استراتيجيّة الهجمات السيبرانيّة الأمريكيّة متأثّرة بالأولويّات الجديدة للصناعة العسكريّة الإسرائيليّة، المصنّفة بالبالغة السريّة، والتي تستهدف تباعًا الصناعة النوويّة الإيرانيّة[22]، والصناعات الدفاعيّة الأوروبيّة المفترض أنّها تعود لبلدان حليفة، ولا تزال. وفي الجهة الأخرى من العالم، كانت هناك توجّهات للخصم التقليديّ، ونقصد به روسيا الاتحاديّة[23]؛ فقد كانت الأسبق في نطاق الاستعداد للهجمات السيبرانيّة. ولقد قامت بعض دول العالم بالفعل نفسه في السنوات الأخيرة، وعملت على تطوير استخدام مهارات الإنترنت والحواسيب كأدوات هجوم ودفاع واستخبارات وحروب نفسيّة. فقد أنشأت كلّ من بريطانيا وفرنسا وكوريا الجنوبيّة وحدات خاصّة في قوّاتها المسلّحة مسؤولة عن الحرب الإلكترونيّة أو حرب المعلومات. وفي مايو 2009، أدخلت شركة American Security اسم إيران بين الدول الخمس التي تتمتع بأقوى قدرات إنترنت في العالم؛ وتجمع هذه الوحدات الخاصة ما بين العقل العسكري والمهارات التقنية التي تمكّنها من الدفاع وصدّ الهجمات أو إحداث خسائر.

---

[21] – فرد كابلان، ترجمة لؤي عبد المجيد، المنطقة المعتمة: التاريخ السريّ للحرب السيبرانية، عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، 2019.

[22]– المركز الاستشاري للدراسات والتوثيق، " التحوّلات في العقيدة العسكرية الأمريكية: دعائم الضعف السبع"، أوراق استراتيجية، سلسلة غير دورية تُعنى بالشؤون الاستراتيجية، العدد2، أيلول 2014، بيروت، ص 17.

[23] –Keir Giles, "Information Troops a Russia Cyber Command?" legal paper third international conference on Cyber Conflicts, Tallinn Estonia,2011,p.47.

من ناحية أخرى، يتزايد استخدام الإنترنت بشكلٍ عام، ووسائل التواصل الاجتماعيّ بشكلٍ خاص، كأداة فعّالة في الحرب التي تشنّها التنظيمات المسلّحة، ولا سيّما في الشرق الأوسط. فقد وجدت هذه المجموعات في الفضاء الإلكترونيّ وسيلة مفيدة في صراعها، فاستخدمت وسائل التواصل الاجتماعيّ لتجنيد المقاتلين؛ كما استفادت هذه التنظيمات من الفضاء الإلكترونيّ كمنصّة لإطلاق الحرب النفسيّة ضدّ الخصوم، بتصوير مشاهد العنف ونشرها على نطاق واسع لبثّ الرعب والذعر.

وعليه، نجد أنّ العديد من الدول، اليوم، تصرف المليارات على الأنشطة السيبرانيّة استعدادًا لحروب المستقبل، حيث تبني استراتيجيّات حرب المعلومات، والتي يتمّ خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القرار لدى الخصوم، عبر اختراق أنظمتهم، واستخدام معلوماتهم ونقلها حتى لا تذهب الحروب لمصلحة من يملك القوّة فقط، وإنّما القادر على شلّ القوّة، والتشويش على المعلومة، بل ربما تغيير البيئة الثقافيّة والفكريّة للخصوم والتأثير فيها قدر الإمكان.

ب-نماذج عن الهجمات السيبرانيّة:

يُسجّل لنا التاريخ المعاصر نماذج للهجمات السيبرانيّة، سوف نأتي على ذكر بعضها فقط، وأوّلها الهجوم السيبرانيّ الذي نفّذته الولايات المتحدة الأمريكيّة وصرّحت به عام 1982 ضدّ منظومة التحكّم العالية صناعيًّا في أنبوب نفط (Chelyabinsk) التابع للاتحاد السوفياتي السابق، وهو ما نفاه الاتحاد السوفياتي السابق آنذاك[24].

أمّا النموذج الآخر، فهو ما تعرضت له أنظمة الاتصال الإلكترونيّة التابعة لوزارة الدفاع الأمريكي (Pentagon)، ووكالة الفضاء الأمريكيّة (NASA)، ووكالة الطاقة الأمريكيّة (Energy-Department)، من هجمات سيبرانيّة بين العامين 1998 – 2000، والذي أدّى إلى الاستحواذ على الآلاف من الملفات المصنّفة بأنّها عالية السريّة. وقد وجهت الولايات المتحدة التهمة رسميًّا إلى روسيا الاتحاديّة، في حين أنكرت الأخيرة -آنذاك- مسؤوليّتها عن هذا الهجوم.

وفي كانون الثاني من العام 2017، كشف تقرير لوكالة الاستخبارات الأمريكيّة عملية قرصنة على الانتخابات الرئاسيّة الأمريكيّة الأخيرة، حيث أفاد التقرير «أنّ الرئيس الروسي فلاديمير بوتين أمر بحملة تأييد لمصلحة الرئيس ترامب، خلال الانتخابات»، وأوضح «أنّ الروس حاولوا تقويض إيمان المواطنين بالعملية الديمقراطية الأمريكيّة، وتشويه سمعة الوزيرة هيلاري كلينتون، والتأثير في حظوظها الانتخابيّة»، وذلك، حسب التقرير، بسبب رغبة روسيا في تقويض النظام الديمقراطي الحر الذي تقوده

[24] Diego Rafael Canabarro and Thiago Borne," Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper No.13:001, March 1, 2013, footnote 11, p.10

الولايات المتحدة الأمريكية. وهذه العمليات الروسية باتت أكثر تصعيدًا في مباشرتها ومستوى نشاطها وسِعَة جهودها، إذا ما قورنت بعمليّاتها السابقة.

وقد تكون أكثر الهجمات حداثةً ما تقوم به الولايات المتحدة و«إسرائيل» بشأن البرامج النوويّة الإيرانيّة، إذ شنّت الولايات المتحدة، قبيل أعوام من توصل المجتمع الدولي إلى الاتفاق النووي مع طهران (2015)، حربًا سيبرانيّة على مشروع إيران النووي، بهدف إضعاف قدراتها النووية، وإجبارها على التنازل على طاولة المفاوضات.

لكنّ الولايات المتحدة نفسها لم تكن بمأمن من الحرب السيبرانيّة. ففي العام 2018، وجّهت وزارة العدل الأمريكيّة اتهامات جنائيّة، وفرضت عقوبات على شركة إيرانيّة و9 إيرانيّين ناشطين في معهد «مبنا» الإيرانيّ، لاختراقهم أنظمة مئات الجامعات والشركات، بهدف سرقة البحوث والبيانات الأكاديمية والملكيّة الفكريّة. وكانت إيران قد استهدفت الأنظمة الإلكترونيّة لشركة نفط أرامكو عام 2017، حيث أجبرت قوة الهجوم السلطات على استبدال مجمل الشبكة الإلكترونيّة التي تعمل عليها الشركة، وتبع ذلك تغيير كثير من الأجهزة العاملة[25]. فهل الحرب السيبرانيّة هي أكثر ميدان مرشّح للتصاعد خلال المرحلة القادمة بين الولايات المتحدة وإيران؟ ولا سيّما أنّ هناك تعاملًا متبادلًا بين إيران وروسيا من جهة وإيران والصين من جهة أخرى؛ وروسيا[26] والصين[27] تُعدّان من «الطبقة الأولى» في امتلاك

---

[25] –https://jawalmax.com/learn-about-the-highlights-of-2018-and-2019-cyber-attacks/

[26] – تستخدم روسيا **غلوناس**، وهو نظام للملاحة بالأقمار الاصطناعية مبني على الراديو، يُدار بواسطة قوات الفضاء الروسية لحساب الحكومة الروسية. وهو نظام بديل ومكمّل لنظام التموضع العالمي (GPS) الأمريكي. بحلول عام 2010، حقّق غلوناس تغطية بنسبة 100٪ لأراضي روسيا. في 26 يوليو 2019، وافق البرلمان الروسي على اتفاقية للتعاون في استخدام نظام غلوناس مع نظام بايدو الصيني.

[27]– تستخدم الصين نظام **بايدو BeiDou** للملاحة بالأقمار الصناعية. هو نظام صيني للملاحة بالأقمار الصناعية. يتكون النظام من مجموعتين من الأقمار الصناعية – واحدة مخصّصة للاختبار المحدود تعمل منذ 2000، والثانية تمثّل نظامًا كاملًا للملاحة، وهي حاليًا قيد التكوين. سيكون نظامًا عالميًا للملاحة بالأقمار الصناعية، يتكوّن من 35 قمرًا صناعيًا، وهو قيد الإنشاء ابتداءً من يناير 2013. أصبح النظام عاملًا في الصين في ديسمبر 2011، مستخدمًا 10 أقمار صناعية، وبدأ في تقديم خدمات الملاحة للمستخدمين في منطقة آسيا–المحيط الهادئ في ديسمبر 2012، ومن المخطط أن يوفّر خدمات الملاحة على مستوى عالمي عند اكتمال بناء النظام في 2020. إن الدافع الأصلي للملاحة الفضائية هو استخدامها في التطبيقات العسكرية حيث توفر الملاحة عبر الأقمار الصناعية دقةً في إيصال الأسلحة إلى الأهداف المطلوبة، مما يزيد بشكلٍ كبير من فتكها، مع تقليل الإصابات غير المقصودة من الأسلحة غير الموجّهة بشكلٍ صحيح. وتسمح الملاحة عبر الأقمار الصناعية أيضًا بتوجيه القوات وتحديد مواقعها بسهولة أكبر، مما يقلّل من ضباب الحرب.

القدرات الإلكترونيّة والهجمات السيبرانيّة. كما أنّ القدرات الفنيّة للقوّات السيبرانيّة الإيرانيّة أصبحت واضحة جدًا، حيث تمكنت من التسلل مرارًا إلى الحكومات الغربيّة وشبكات الاستخبارات الإقليميّة. فعلى الرغم من كلّ الإجراءات الأمنية التي تم اتخاذها في ديسمبر 2011، أشار المدير التنفيذي لشركة Google ، إريك شميدت، في مقابلة مع شبكة CNN الأمريكيّة، إلى أنّ الإيرانيّين موهوبون على نحو غير معتاد في الحروب السيبرانيّة الحديثة، وذلك لأسباب لا تفهمها الولايات المتحدة.

وفي الآونة الأخيرة، وتحديدًا في نيسان من العام 2020، أعلنت «إسرائيل» عن هجوم سيبرانيّ استهدف شبكات المياه الخاصة بها. واتهم الإسرائيليّون ايران بالمسؤوليّة عن الهجوم، في حين أنّ «إسرائيل» والولايات المتحدة الأمريكيّة قد أطلقتا أكثر من فيروس لاستهداف المنشآت النوويّة الإيرانيّة، وآخرها ما وقع في شباط وأيار وتموز من العام 2020، بحيث أقرّ وزير الأمن الإيراني «محمود علوي» بأنّ هناك أكثر من مليوني هجوم سيبراني وقع بين عامي 2019 و2020. وبحسب وزير الأمن، فإنّ «إسرائيل» وأمريكا والسعودية مصدرها، علمًا أنّ الأخيرة تعمل على تدريب 5000 عنصر في البانيا لهذا الغرض.

ويمكن القول في ضوء تلك النماذج، إنّه بالرغم من اختلاف غرض كلّ حالة من الحالات السابقة وهدفها، فإنّه من الواضح أنّ حجم الهجمات السيبرانيّة يتزايد بشكل حاد. ولذا يصعب تحديد حجمها الحقيقي، وبخاصّة أنّ العديد منها لا يتمّ التبليغ عنه. وتتمثّل القواسم المشتركة بين تلك الحالات في صعوبة تحديد مُرتكبي تلك الهجمات على وجه الدقّة، وغياب الردّ المضاد كنتيجة لها؛ والأهمّ أنّها ليست حكرًا على الدول المتقدّمة ذات أنظمة المعلومات الهائلة والمتطوّرة فحسب. وعليه، نرجّح بأنّ حروب المستقبل حتمًا ستكون حروبًا سيبرانيّة، أو على الأقلّ في جزء منها، حيث إنّ الفضاء السيبرانيّ قد وِسِم رسميًّا على أنّه «ميدان» للحرب، مثل الجوّ، والبرّ، والبحر، والفضاء الخارجيّ. ونظرًا إلى سلاسة الشبكة الحاسوبيّة العالميّة وانسيابيّتها، وبسبب حزم البيانات، وإنترنت الأشياء، فإنّ الحرب السيبرانيّة لن تشتمل على الجنود، والبحارة، والطيّارين فقط؛ ولكنّها، حتمًا ستتضمّن البقيّة منّا، فحينما يكون الفضاء السيبرانيّ في كلّ مكان، فإنّ الحرب السيبرانيّة يمكن أن تتسرّب وتتضح عبر كلّ المسام الرقميّة.

خامسًا: العمليّات السيبرانيّة: بين الأمن والردع

الآن، تُستخدم أنظمة الأقمار الصناعية للملاحة العالمية لتحديد موقع المستخدمين وموقع الأشخاص أو الأشياء الأخرى، في أي لحظة معيّنة. ويُعد نطاق تطبيقات الأقمار الصناعية في المستقبل هائلًا، وهو يشمل القطاعين العام والخاص عبر العديد من قطاعات السوق، مثل: العلوم، والنقل، والزراعة. وكما أنّ القدرة على توفير إشارات الملاحة عبر الأقمار الصناعية تعني القدرة على رفضها. يُحتمل أن يكون لدى مشغّل نظام الملاحة عبر الأقمار الصناعية القدرة على تقليل أو إزالة خدمات الملاحة عبر الأقمار الصناعية فوق أي إقليم يرغب فيه.

الأمن السيبرانيّ (cybersecurity) مصطلح حديث، ويُطلق عليه أيضًا «أمن المعلومات»، و«أمن الحاسوب»[28]؛ وهو فرع من فروع التكنولوجيا يُعنى بممارسة حماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقميّة التي تهدف عادة للوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها، أو ابتزاز المال من المستخدمين، أو تعطيل العمليات. ويُعرّفه «إدوارد أموروسو» (Edward Amoroso) بأنّه «مجموع الوسائل التي من شأنها الحدّ من خطر الهجوم على البرمجيّات أو أجهزة الحاسوب أو الشبكات. وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات الرقميّة ووقفها، وتوفير الاتصالات المشفرة»[29].

ومن هنا نجد أنّ ظهور الأمن السيبرانيّ ارتبط بظهور الهجمات السيبرانيّة كونها باتت تشكل خرقًا للأمن القومي[30]. وهذا بسبب تأثير التكنولوجيا في المفاهيم ذات الصلة، كالقوّة power، والسيادةsovereignty . والحوكمة العالميّة global governance والأمننة securitization، ونظرًا إلى طبيعة الفضاء السيبرانيّ، حيث إنّه ساحة عالميّة عابرة لحدود الدول، تمتدّ قضية الأمن السيبرانيّ من داخل الدولة إلى مجموعة النظام الدولي، ومع وجود مخاطر تهدّد الفاعلين جميعًا في مجتمع المعلومات العالمي، تصبح القضية مرتبطة بالأمن العالمي. ومن هنا كانت المحاولة الأولى لوضع معاهدة دوليّة لمراقبة الفضاء السيبرانيّ وما يتصل به في العام 2001؛ وقد أسهمت اللجنة الدوليّة للصليب الأحمر، بصفتها مراقبًا، في نشر ما يُعرف بـ«دليل تالين للقانون الدولي المُطبَّق على

---

[28] – بيْد أنّ هناك من وجد فرقًا واضحًا بين أمن المعلومات والأمن السيبراني، والذي يتمثل في اختلافات معروفة، وهي: بالنسبة إلى الأمن السيبراني: يقوم بحفظ كل الأجهزة الإلكترونيّة التي يتم حفظ البيانات والمعلومات المهمة عليها والدفاع عنها؛ وبالتالي يتم تخزين المعلومات دون التعرض إلى أي اختراق أو سرقة، عن طريق استخدام أشهر البرامج المتخصصة في هذا العمل بكفاءة. يُعدّ هذا الأمن من الأسلحة المتطورة الموجودة في الدول المختلفة، حيث تسعى معظم هذه الدول إلى الدفاع وحماية هذا الاختراع المهم من السرقة والاختراق، حيث يحمي المعلومات الخطيرة والمهمة التي لها علاقة بأمن وسياسة البلاد ويخزّنها. بالنسبة إلى أمن المعلومات: يضع أمن المعلومات تركيزه الكامل على المعلومات المحفوظة على الحواسيب والأجهزة الإلكترونيّة الأخرى، ولا يهتم بشيء آخر، حيث اهتمامه يدور حول المعلومات الفيزيائية فقط، وبذلك يكون معاكسًا للأمن السيبراني.

[29] –https:// hbrarabic.com

[30] – قدرة الأمّة على الدفاع عن أمنها، وحقوقها، وصياغة استقلالها، وسيادتها على أراضيها، وتنمية القدرات والإمكانات، في مختلف المجالات السياسية، والاقتصادية، والثقافية والاجتماعية، مستندة إلى القدرة العسكرية، والدبلوماسية، آخذة في الاعتبار الاحتياجات الأمنية الوطنية لكل دولة، والإمكانات المتاحة، والمتغيرات الداخلية، والاقليمية، والدولية، والتي تؤثر على الأمن القومي.

الحرب الإلكترونيّة»[31].هذ بالإضافة إلى بروز اتجاهات متعدّدة لتحقيق هذا الأمن، وذلك عبر التنسيق بين أصحاب المصلحة من الحكومات، والمجتمع الأهلي، والشركات التكنولوجيّة، ووسائل الإعلام، وغيرها، للحفاظ على خصوصيّة الفرد وحريّته وتفكيره وحقّه في حفظ بياناته من دون اختراق. وقد بات الأمن السيبرانيّ يشكّل جزءًا أساسيًّا من أيّ سياسة أمنيّة وطنية، حيث بات معلومًا أنّ صنّاع القرار في الولايات المتحدة الأمريكيّة، الاتحاد الأوروبي، روسيا، الصين، إيران وغيرها من الدول، أصبحوا يصنّفون مسائل الدفاع السيبرانيّ/ الأمن السيبرانيّ كأولويّة في سياساتهم الدفاعيّة الوطنية؛ هذا بالإضافة الى تشييد قوّة سيبرانيّة تقوم بالهجوم من خلال برمجيّات خاصّة، فنجد أنّ أغلب الجيوش في العالم تمتلك وحدة أمن إلكترونيّ ووحدة أمن الدفاع عن الهجمات السيبرانيّة؛ لذا نجد أنّ الأمن المعلوماتيّ لم يعد حكرًا على الشركات أو المؤسسات صاحبة العلاقة، بُغية حفظ البنوك ومعطياتها من أيّ استهداف، بل أضحى أيضًا يشكّل رهانًا قويًّا وتحديًّا كبيرًا بوجه الدول والحكومات، بحيث تحوّلت وحدة الأمن الإلكترونيّ إلى قيادة قتالية منفصلة عند الدول الكبرى.

وهنا تتجلّى استراتيجيات المواجهة لتطرح إشكاليّة مدى إمكانية تحقيق الردع السيبرانيّ لمنع الأعمال الضارّة ضدّ الأصول الوطنيّة في الفضاء، والذي يرتكز على ثلاث ركائز هي: مصداقية الدفاع، والقدرة على الانتقام، والرغبة فيه[32].ولعلّ ما شهده الواقع المعاصر من حالات متباينة تطال الدول المتقدمة والنامية على حدّ سواء، يؤكّد تلك الحاجة ويعزّزها. ولكن إلى أيّ مدى يمكن ردع تلك الهجمات، وما طبيعة التحدّيات التي تعترض ذلك المدى؟

سادسًا: تحدّيات الردع السيبرانيّ

تواجه عمليّة الردع السيبراني تحدّيات أبرزها:

أوّلًا: الإسناد (تحديد مُرتكب الهجمات بدقّة). من شأن الردع السيبرانيّ أن يفشل طالما لم يعلن الجاني رسميًا عن مسؤوليّته عن الهجوم؛ اذ يمكن لأيّ شخص أن يكون هو الجاني في الهجمات

---

[31] – وهو وثيقة غير مُلزمة شاركت في صياغتها مجموعة من الخبراء القانونيين والعسكريين من عدة دول. و«الحرب السيبرانية»، وفق دليل تالين، هي «وسائل وأساليب القتال التي تتألف من عمليات في الفضاء الإلكترونيّ ترقى إلى مستوى النزاع المسلّح أو تُجرى في سياقه»، ضمن المعنى المقصود في القانون الدولي الإنساني. أما «الهجوم السيبراني»، فيُعرّفه الدليل بالاستناد إلى القانون الدولي الإنساني، «بأنّه عملية إلكترونيّة سواء هجومية أو دفاعية يُتوقّع أن تتسبّب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها».

[32]–أندريه بوفر، *الردع والاستراتيجية*، ترجمة: أكرم ديري، بيروت: دار الطليعة للطباعة والنشر، 1970، ص. 31.

السيبرانيّة، وبخاصّة أنّ المعدات اللازمة لشنّ هجوم سيبرانيّ يمكن الوصول إليها، وليست مكلفة، ويمكن شنّها من أيّ مكان تتوافر فيه خدمة الإنترنت؛ فلكي يعمل الردع لا بدّ من أن يقلق المهاجم من كشف هويّته، ومن ثمّ تعرّضه للعقاب أو الانتقام. بيْد أنّ صعوبة تحديد مرتكب الهجمات بدقّة قد تسفر عن استهداف طرف ثالث لا علاقة له بالهجوم الأولي، وهو الأمر الذي لا يُضعف فقط من منطق الردع وفلسفته، لكنّه يخلق عدوًا جديدًا أيضاً. فعدم التغلب على تلك الإشكالية يعني تكرار الهجمات مرّة أخرى دون تعرّض المهاجم للعقاب؛ أو بعبارة أخرى، تحسين سُبل الإسناد ضرورة لفعاليّة الردع.

ثانيًا: العقوبات القانونيّة التي لا يمكن تطبيقها حاليًّا على الهجمات السيبرانيّة إلّا بشكل غير مباشر، لأنّ جرم القانون الدولي منسوب إلى العدوان العسكري. ولكن ماذا عن الهجوم السيبرانيّ الذي أسفر عن انفجار قاعدة عسكريّة؟ وهل يحقّ للدولة – إعمالًا لحقّها الأصيل في الدفاع عن النفس – استهداف أهداف عسكريّة ضدّ تلك الدولة أو حتى شنّ هجوم سيبرانيّ مضاد؟! لا يزال النقاش دائرًا حول المسائل القانونيّة المتعلقة بالهجمات السيبرانيّة. وعليه، قد يبدو الردّ الانتقامي عملًا عدوانيًا غير مبرّر أو مخالفًا لقواعد القانون الدوليّ[33].

ثالثًا: الفاعلون من غير الدول الذين يمكن لهم إحداث أضرار بدرجات مختلفة، ما يُضفي مزيدًا من التعقيد على الردع السيبراني نظرًا إلى صعوبة استهداف هؤلاء الفاعلين. وهنا المقصود المنظمات الإجراميّة، والجماعات الإرهابيّة، والنشطاء السياسيّون، وغيرهم، ما يدعو إلى التساؤل عن جدوى الرد الانتقامي؛ ماذا إذا وُجد هذا الفاعل داخل دولة ما، ووفّرت له دولة أخرى الحماية، أيّهما تتحمّل المسؤوليّة؟

رابعًا: المصداقيّة، فهي غير متوفرة في الفضاء السيبرانيّ لكلا الجهتين، بسبب عدم توفر إسناد الهجوم إلى مرتكبيه من جهة، ولأنّ الأسلحة السيبرانيّة خفيّة وغير مرئيّة إلى أن يُقدم طرف ما على استخدامها. ولذلك، لا يمكن للمهاجم أن يعرف إذا امتلك الخصم القدرة على الردّ أو الانتقام هذا من جهة ثانية[34].

---

[33] MAJ Lee Hsiang Wei, The Challenges of *Cyber Deterrence, Journal of the Singapore Armed Forces, Vol. 41, No. 1, 2015, p. 13-22.*

[34] Haylen Cohen, *The Approaches and Limitations of Cyber Deterrence*, Fall 2005, http://www.cs.tufts.edu/comp/116/archive/fall2015/hcohen.pdf

ولا يمكن تجاهل ثغرة اتساع مفهوم الردع السيبرانيّ، حيث إنّه يطال مجالات عدّة مثل: الاتصالات، والتجارة، والأعمال التجارية، والتعليم، والتدريب، وأكثر من ذلك. لذا، بناء استراتيجيّة فاعلة للردع في الفضاء السيبرانيّ يتطلب تجاوز الحديث عن المجال ككلّ إلى الحالات التي يمكن للردع أن يكون فاعلًا فيها؛ إلّا أنّ الحديث اليوم عن الردع السيبرانيّ بات أكثر مرونة، وذلك من خلال مقاربات مختلفة، ويمكن تداولها بخيارين مختلفين:

– الخيار الأوّل: استخدام الأنظمة البديلة: وذلك يكون من خلال اعتماد الدولة أنظمة بديلة، وليس الاعتماد على نظام واحد يُخترق بسهولة، ما يؤدّي إلى نتائج وخيمة؛ وبخاصّة إذا تعلق هذا النظام بالبنية التحتية الرئيسة للدولة. وهذا يمكّن الدولة من استخدام خيارات أخرى في حال تعرّضها لهجوم سيبرانيّ، بحيث تلجأ إلى الاستعانة بتلك الأنظمة البديلة أو الاحتياطيّة.

الخيار الثاني: إعادة التأسيس: **وهذا يعتمد على التوقيت**؛ فإذا تمكّنت الدولة من التغلب على الهجوم الذي تتعرّض له بسرعة، وإعادة تشغيل النظام، ستكون الآثار هامشيّة. ولكن الطريقة الوحيدة لتجنّب الهجوم هي الاحتجاب عن الجميع. وبالرغم من كونه السبيل الأفضل للردع، فإنّه يكتنفه مسائل قانونيّة عدّة.¨

الخاتمة

نعيش اليوم واقعًا عالميًّا جديدًا يتميّز بكثير من التعقيد، حيث يبدو الفضاء السيبرانيّ مسرحًا للنزاع وكأنّه تصعيد للخصائص التي حوّلت الحروب بالوكالة إلى الخيار المفضّل للفاعلين الذين يريدون تعزيز مصالحهم مقابل القليل من المخاطر. فمن جهة، يتمّ الانطلاق من فكرة أنّ هذا الوسط التقنيّ الجديد يخلق حافزًا قويًّا لدى الأطراف لتسوية نزاعاتها بطريقة تصادميّة؛ ومن جهة أخرى، يُفترض أنّ عدم وضوح الهويّة وصعوبة إلقاء المسؤوليّات عند وقوع هجوم سيبراني يوفّران مستوى عاليًا من «الإنكار المُقْنع»، ما يشيع الافتراض بسهولة الدخول في نزاعات سيبرانيّة، بسبب الكلفة الاقتصاديّة

الضئيلة التي يتطلبها تطوير القدرات السيبرانيّة. وعلى المنوال ذاته، أدّى توسع النفاذ إلى التقنيات الجديدة والطابع الديمقراطي لانتشارها إلى ظهور عدد كبير جدًّا من الفاعلين الذين يُعتمد عليهم من أجل تقويض مواقف الخصوم، وبتنا أمام مصطلحات حربيّة تقليديّة تُضاف إليها الصفة الافتراضيّة التخيليّة، السيبرانيّة، أو الرقميّة أو الإلكترونيّة، مثل: التسليح الإلكترونيّ، سباق التسلّح الإلكترونيّ، ساحات الحرب الإلكترونيّة، الجيش الإلكترونيّ، الهجوم السيبرانيّ، الجهاد الإلكترونيّ، المحاربون أو المقاتلون الإلكترونيّون، المناورات الإلكترونيّة؛ وأخيرًا الإرهاب السيبرانيّ. وهذا ما دفع مجموعة من الدول إلى المطالبة بعقد اتفاقية دولية للحدّ من التسلّح داخل الفضاء الإلكترونيّ، كتلك التي تمّت في مجال الانتشار النووي والكيماوي، بحيث يمكن لهذه الاتفاقيات أن تُسهم – في حال تطبيقها – في وضع قيود على الحروب الإلكترونيّة، واستخدامها وتوزيعها وانتشارها وتطويرها، إذ يشكّل ارتباط البنى التحتية الخاصة بتقنيات المعلومات والاتصالات، كما الاعتماد المتزايد عليها من الدول والأفراد والمؤسّسات، عاملًا محفّزًا لتصاعد نسبة المخاطر، ما يفرض اتخاذ تدابير وإجراءات، تضمن إدارة فاعلة للمخاطر التقنية والسيبرانيّة، تعتمد على منهجية تتناسب والأبعاد الواسعة لهذا الارتباط، ما ينسحب على البلدان أجمع. لذلك، لا بدّ من أن تنطلق الحلول في هذا المجال من فهم الطبيعة الخاصة لتقنيات المعلومات والاتصالات، سيّما الجزء الخاص بتجاوزها الحدود، والمجتمعات، والأنظمة، كما لطبيعة البنى التحتية نفسها.

ويبقى القول إنّ كلّ دولة عليها واجب اتخاذ التدابير المعقولة والمناسبة لتأمين مجتمع المعلومات. فإنّ طبيعة العمليات السيبرانية تُقوّض من الدور المحتمل للردع، وقد تجعله عديم الفائدة كليًا. فتعرُّض دولة ما لهجوم يضرّ باقتصادها وبُناها التحتية أو بأرواح مواطنيها، من دون أن تعرف مصدره ولا دوافع تنفيذه، أمرٌ ذو فائدة ردعية ضئيلة؛ فإنّ إخفاء الهويّة بشكل مطلق، بحيث لا يمكن حتى التوصل إلى تحميل المسؤولية لطرف ما على نحو تخمينيّ، قد يكون مشكلة للمهاجِم أكثر من المدافع. فالتقنيّة لم تغيّر الطبيعة السياسيّة للحرب، التي صاغها **كارل فون كلاوزفيتز** في زمنه، حين وصفها بأنّها «عمل قسري موجّه إلى عدو» (بغضّ النظر عن وسيلة تنفيذه)، وهي ما زالت عملًا موجّهًا إلى فاعل معيّن لكي يغيّر سلوكه وفقًا لإرادة آخر. والاستخدام المجرّد للعنف (المادي أو الرمزي) إذا لم يُصاحبه ما يدلّ على أسباب استعماله، ويوضح شروط توقفه، يصعب جدًّا أن يُسهم في تحقيق أهداف من يلجأ إليه[35]. وبالرغم من ذلك، تتزايد أهمية الردع في ظلّ

[35] https://www.aljazeera.net/midan/reality/politics –

هشاشة الدول في الاستجابة للهجمات السيبرانيّة التي تزداد خطورة متى قابلها قلّة وعي وإدراك، لأساليب وطرق الوقاية .

وختاماً، يمكن طرح التساؤلات الآتية: هل فرض العقوبات، والتشديد بالإجراءات القانونيّة الرادعة، وتطوير ونشر قدرات دفاعيّة، يؤدّي إلى منع نجاح أي هجوم محتمل؟ أم إنّ إنشاء قوات متخصصة للمهمات السيبرانيّة، وتطوير البنية التحتيّة العسكريّة والتجارية المهمة وتعزيزها، تصدّ أيّ هجوم محتمل؟ وهل تعزيز الاستخبارات وتطويرها لاكتشاف هويّة المهاجم يكفي لبناء استراتيجيّة ردع سيبراني؟ أم أنّ الأمر يتطلب الاعتماد على الأسلحة غير النوويّة، على نطاق واسع، مثل: الضربات التقليدية والدفاع الصاروخي، والفضاء الهجومي في ظلّ ما يراه بعضهم عن عدم إمكانيّة الهجمات السيبرانيّة من تحقيق أهداف ذات طبيعة استراتيجيّة!

المراجع

<u>باللغة العربية</u>

1- فرد كابلان، ترجمة لؤي عبد المجيد، المنطقة المعتمة: التاريخ السري للحرب السيبرانية، عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، 2019.
2- المركز الاستشاري للدراسات والتوثيق، " التحولات في العقيدة العسكرية الأمريكية: دعائم الضعف السبع"، أوراق استراتيجية، سلسلة غير دورية تُعنى بالشؤون الاستراتيجية، العدد2، أيلول 2014، بيروت.
3- أندريه بوفر، *الردع والاستراتيجية*، ترجمة: أكرم ديري، بيروت: دار الطليعة للطباعة والنشر، 1970.
4- دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها" ، فيينا عام 2013 ، الوثيقة:UNODC/CCPCJ/EG.4/2013/2
5- لورنس لسيج، الكود المنظّم للفضاء الإلكترونيّ، ترجمة: محمد سعد طنطاوي ، ط 2 (القاهرة : مؤسسة هنداوي للتعليم والثقافة ، 2006).
6- منير البعلبكي،" المورد: قاموس إنكليزي –عربي"، دار العلم للملايين، بيروت، 2004.

باللغة الاجنبية

1. Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University Press, 2010.
2. Norbert Wiener, "Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.
3. Richard Kissel, “Glassory of Key Information Security Terms", National Institute of Standards and technology, U.S Department of Commerce 2013.
4. James A. Lewis, "Sovereignty and the role of Government in Cyberspace", Center for Strategic and International Studies Journal, Spring Summer, Vol: XVI, Issue II, 2010.
5. Shin, Beomchul," The Cyber Warfare and the Right of Self –Defense: Legal Perspectives and the Case of the United States, IFANS, Vol.19, 2011.
6. K.Saalbach," Cyber War, Methods and Practice", Version 9.0, University of Osnabruck-17 ,2014.
7. Michael Gervais, “Cyber Attacks and the Laws of War", Berkeley Journal of International Law", Vol: 30, Issue .2, Article 6, 2012.
8. Joseph S.Nye JR , Cyber Power, Harvard Kennedy School, 2010.
9. Edward J. Glantz, “Guide to Civil War Intelligence,” The Intelligencer: Journal of U.S. Intelligence Studies, 2011.
10. David Kahn, The Codebreakers (New York: Scribner; rev. ed., 1996)

11. MAJ Lee Hsiang Wei, The Challenges of *Cyber Deterrence, Journal of the Singapore Armed Forces, Vol. 41, No. 1, 2015.*
12. Keir Giles, "Information Troops a Russia Cyber Command?" legal paper third international conference on Cyber Conflicts, Tallinn Estonia,2011.
13. Diego Rafael Canabarro and Thiago Borne," Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper, 2013.

المواقع الإلكترونيّة

-http://www.cs.tufts.edu/comp/116/archive/fall2015/hcohen.pdf

-https://www.aljazeera.net/midan/reality/politics -

-https:// hbrarabic.com

-https://jawalmax.com/learn-about-the-highlights-of-2018-and-2019-cyber-attacks/